○相楽東部広域連合情報セキュリティ対策要綱

令和３年８月１日

要綱第１号

目次

附則

第１章　総則及び組織・体制

（目的）

第１条　この要綱は、相楽東部広域連合情報セキュリティに関する規則（令和３年規則第３号）に基づき、相楽東部広域連合（以下「本連合」という。）における情報セキュリティ対策の具体的な遵守事項及び判断基準等を定めることを目的とする。

（情報セキュリティ委員会）

第２条　本連合における情報セキュリティに関する最高意思決定は、相楽東部広域連合情報セキュリティ委員会（以下「委員会」という。）が行う。

２　委員会は、次の事項を審議する。

(1)　規則及び要綱の運用及び見直しに関する事項

(2)　情報セキュリティに関する事案の調査に関する事項

(3)　情報セキュリティ監査の実施手順等に関する事項

(4)　その他情報セキュリティに係る重要事項に関する事項

３　委員会は、総務課長、環境課長、学校教育課長及び生涯学習課長（以下「課等の長」という。）をもって構成する。

４　委員会の長は、次条に定める最高情報セキュリティ責任者とする。

５　委員会の事務は、総務課が行う。

６　委員会は必要に応じて、情報セキュリティ対策の監査作業を行う「情報セキュリティ監査チーム」等の「専門チーム」を編成することができる。

（最高情報セキュリティ責任者）

第３条　本連合に「最高情報セキュリティ責任者」（以下「CISO」という。）を置く。

２　CISOは、事務局長をもって充てる。

３　CISOは、本連合における全てのネットワーク、情報システム等の情報資産の管理並びに情報セキュリティ対策に関する最終決定権限及び責任を有する。

４　CISOは、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めることができる。

（統括情報セキュリティ責任者）

第４条　本連合に「統括情報セキュリティ責任者」を置く。

２　統括情報セキュリティ責任者は、総務課長をもって充て、CISOを補佐するものとする。

３　統括情報セキュリティ責任者は、本連合の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

４　統括情報セキュリティ責任者は、本連合の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

５　統括情報セキュリティ責任者は、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

６　統括情報セキュリティ責任者は、本連合の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合にCISOの指示に従い、CISOが不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

７　統括情報セキュリティ責任者は、本連合の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

８　統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括情報セキ

ュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者を網羅する連絡体制を含めた緊急連絡網を必要に応じて整備しなければならない。

9　統括情報セキュリティ責任者は、緊急時にはCISOに早急に報告を行うとともに回復のための対策を講じなければならない。

(情報セキュリティ管理者)

第5条　本連合に「情報セキュリティ管理者」を置く。

2　情報セキュリティ管理者は、課等の長をもって充て、その所管組織の情報セキュリティ対策に関する権限と責任を有するものとする。

3　情報セキュリティ管理者は、所管組織において情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、統括情報セキュリティ責任者及びCISOへ速やかに報告を行い、指示を仰がなければならない。

(情報システム管理者)

第6条　統括情報セキュリティ責任者は、情報システムの運用、管理を行う「情報システム管理者」を指名し、情報システムを適切に管理しなければならない。

2　情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

3　情報システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

4　情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

(情報システム担当者)

第7条　情報システム管理者の指示等に従い、情報システムの設定変更、運用、更新等の作業を行う者を、「情報システム担当者」とする。

(兼務の禁止)

第8条　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

2　監査を受ける者とその監査を実施する者は、やむを得ない場合を除き同じ者が兼務してはならない。

(情報セキュリティに関する統一的な窓口の設置)

第9条　CISOは、情報セキュリティインシデントの統一的な窓口(以下「CSIRT(シーサート)」という。)の機能を有する組織を整備し、情報セキュリティインシデントについて課等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備する。

2　CISOによる情報セキュリティ戦略の意思決定が行われた際には、その内容を関係課等に提供する。

3　情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

4　情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。

第2章　情報資産の管理

第1節　情報資産の分類

第10条　本連合における情報資産は、重要性により次の各号に掲げるとおり分類し、必要に応じ

取扱制限を行うものとする。

(1)　個人情報及びセキュリティ侵害が住民の生命、財産等へ重大な影響を及ぼす情報（以下「重要性Ⅰ」という。）

(2)　公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報（以下「重要性Ⅱ」という。）

(3)　外部に公開する情報のうち、セキュリティ侵害が行政事務の執行等に微妙な影響を及ぼす情報（以下「重要性Ⅲ」という。）

(4)　上記以外の情報（以下「重要性Ⅳ」という。）

第2節　情報資産の管理

（管理責任）

第11条　情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

2　情報資産が複製又は伝送された場合は、複製等された情報資産も前条の分類に基づき、管理しなければならない。

（情報資産の分類の表示）

第12条　本連合の業務に携わる全ての職員及び会計年度任用職員（以下「職員等」という。）は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

（情報の作成）

第13条　職員等は、業務上必要のない情報を作成してはならない。

2　情報を作成する者は、情報の作成時に前条の分類に基づき、必要に応じて当該情報の分類と取扱制限を定めなければならない。

3　情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

（情報資産の入手）

第14条　連合内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

2　連合外の者が作成した情報資産を入手した者は、前条の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

3　情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

（情報資産の利用）

第15条　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

2　情報資産を利用する者は、情報資産の分類に応じて適切な取扱いをしなければならない。

3　情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って当該電磁的記録媒体を取り扱わなければならない。

（情報資産の保管）

第16条　情報セキュリティ管理者及び情報システム管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

2　情報セキュリティ管理者及び情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

3　情報セキュリティ管理者及び情報システム管理者は、重要性Ⅱ以上の情報を記録した電磁的

記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所等に保管しなければならない。

(情報の送信)

第 17 条　電子メール等により重要性Ⅱ以上の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

(情報資産の運搬)

第 18 条　車両等により重要性Ⅱ以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

2　重要性Ⅱ以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

(情報資産の提供・公表)

第 19 条　重要性Ⅱ以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

2　重要性Ⅱ以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

3　情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

(情報資産の廃棄)

第 20 条　重要性Ⅱ以上の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。

2　情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

3　情報資産の廃棄を行う者は、情報セキュリティ管理者の許可を得なければならない。

第 3 章　物理的セキュリティ対策

第 1 節　サーバ等の管理

(機器の取付け)

第 21 条　情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

(機器の電源)

第 22 条　情報システム管理者は、統括情報セキュリティ責任者と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

2　情報システム管理者は、統括情報セキュリティ責任者と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

(通信ケーブル等の配線)

第 23 条　統括情報セキュリティ責任者及び情報システム管理者は連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

2　統括情報セキュリティ責任者及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、損傷等の報告があった場合、連携して対応しなければならない。

3　統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク接続口(ハブのポート等)を適切に管理しなければならない。

4　統括情報セキュリティ責任者及び情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更又は追加できないように必要な措置を施さなければならない。

(機器の定期保守及び修理)

第24条　情報システム管理者は、重要性Ⅱ以上のサーバ等の機器の定期保守を実施しなければならない。

2　情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、外部の事業者に故障を修理させるに当たり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認などを行わなければならない。

(連合外への機器の設置)

第25条　統括情報セキュリティ責任者及び情報システム管理者は、連合外にサーバ等の機器を設置する場合、CISOの承認を得なければならない。また、必要に応じて当該機器への情報セキュリティ対策状況について確認しなければならない。

(機器の廃棄等)

第26条　情報システム管理者は、機器を廃棄・リース返却等をする場合、機器内部の記憶装置から全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

第2節　管理区域の管理

(管理区域の構造等)

第27条　管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための場所(以下「電算設置場所」という。) や電磁的記録媒体の保管庫をいう。

2　統括情報セキュリティ責任者及び情報システム管理者は、電算設置場所の機器等に転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

3　統括情報セキュリティ責任者及び情報システム管理者は、電算設置場所に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

(機器等の搬入出)

第28条　情報システム管理者は、搬入する機器等が既存の情報システムに与える影響について、あらかじめ職員又は委託した業者に確認を行わせなければならない。

2　情報システム管理者は、電算設置場所の機器等の搬入出について職員を立ち会わせなければならない。

第3節　通信回線及び通信回線装置の管理

第29条　統括情報セキュリティ責任者は、連合内の通信回線及び通信回線装置を適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

2　統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

3　統括情報セキュリティ責任者は、一般事務系のネットワークを総合行政ネットワーク(LGWAN)

に集約するように努めなければならない。

4　統括情報セキュリティ責任者は、重要性Ⅱ以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

5　統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

6　統括情報セキュリティ責任者は、重要性Ⅱ以上の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じて回線を冗長構成にする等の措置を講じなければならない。

第4節　職員等の利用する電磁的記録媒体等の管理

第30条　情報システム管理者は、電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

2　情報システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

第4章　人的セキュリティ対策

第1節　職員等の遵守事項

（情報セキュリティポリシー等の遵守）

第31条　職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。

2　情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

（業務以外の目的での使用の禁止）

第32条　職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

（外部における情報処理作業）

第33条　CISOは、重要性Ⅱ以上の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

2　職員等は、本連合のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

3　職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

（支給以外のパソコン等の業務利用）

第34条　職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、情報セキュリティ管理者の許可を得て利用することができる。

2　職員等は、支給以外のパソコン及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

（持ち出し及び持込みの記録）

第35条　情報セキュリティ管理者は、端末等の持ち出し及び持込みについて、記録を作成し、保管しなければならない。

（セキュリティ設定変更の禁止）

第36条　職員等は、パソコン、モバイル端末及びソフトウェアに関するセキュリティ機能の設定を

情報セキュリティ管理者の許可なく変更してはならない。

(机上の端末等の管理)

第 37 条　職員等は、パソコン、モバイル端末、電磁的記録媒体及び個人情報等が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、長時間離席時にはパソコンをスリープモードにして、再起動時にパスワード入力が必要な状態にすることや電磁的記録媒体、個人情報等が記録された文書等が容易に閲覧されないよう扉及び鍵つきの書類棚への保管を行う等、適切な措置を講じなければならない。

(退職時等の遵守事項)

第 38 条　職員等は、異動･退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

(会計年度任用職員への対応)

第 39 条　情報セキュリティ管理者は、会計年度任用職員に対し、採用時に情報セキュリティポリシー等のうち、会計年度任用職員が守るべき内容を理解させ、また、実施及び遵守させなければならない。

2　情報セキュリティ管理者は、会計年度任用職員の採用の際、必要に応じ、情報セキュリティポリシーを遵守する旨の同意書への署名を求めるものとする。

3　情報セキュリティ管理者は、会計年度任用職員にパソコンによる作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

(情報セキュリティポリシー等の閲覧)

第 40 条　情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように共有フォルダ等にデータを置かなければならない。

(外部委託事業者に対する説明)

第 41 条　情報セキュリティ管理者は、ネットワーク及び情報システムの導入・保守等を外部委託事業者に発注する場合､外部委託事業者から再委託を受ける事業者も含めて情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

第 2 節　研修・訓練

(情報セキュリティに関する研修・訓練)

第 42 条　CISO は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

(研修計画の策定及び実施)

第 43 条　CISO は、全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を必要に応じて行わなければならない。

2　研修は、統括情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

(緊急時対応訓練)

第 44 条　CISO は､緊急時対応を想定した訓練を定期的に実施しなければならない｡訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制・範囲等を定め、効果的に実施できるようにしなければならない。

（研修・訓練への参加）

第 45 条　全ての職員等は、定められた研修･訓練に参加しなければならない。

第 3 節　情報セキュリティインシデントの報告

（連合内からの報告）

第 46 条　職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者に報告しなければならない。

2　報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者に報告しなければならない。

3　情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じて CISO に報告しなければならない。

（住民等外部からの報告）

第 47 条　職員等は、本連合が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ管理者に報告しなければならない。

2　報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

3　情報セキュリティ管理者は、当該情報セキュリティインシデントについて、必要に応じて CISO に報告しなければならない。

（原因の究明・記録、再発防止等）

第 48 条　統括情報セキュリティ責任者は、情報セキュリティインシデントを引き起こした部署の情報セキュリティ管理者と連携し、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。

2　統括情報セキュリティ責任者は、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISO に報告しなければならない。

3　CISO は、統括情報セキュリティ責任者から、情報セキュリティインシデントについて報告を受受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

第 4 節　ユーザーID 及びパスワード等の管理

（ユーザーID の取扱い）

第 49 条　職員等は、自己の管理するユーザーID に関し、次の各号に掲げる事項を遵守しなければならない。

(1)　自己が利用しているユーザーID は、他人に利用させてはならない。

(2)　共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

（パスワードの取扱い）

第 50 条　職員等は、自己の管理するパスワードに関し、次の各号に掲げる事項を遵守しなければならない。

(1)　パスワードは、他者に知られないように管理しなければならない。

(2)　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

(3)　パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

(4)　パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

(5)　パスワードは定期的に変更し、古いパスワードを再利用してはならない。

(6)　複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
(7)　仮のパスワードは、最初のログイン時点で変更しなければならない。
(8)　パソコン等の端末にパスワードを記憶させてはならない。
(9)　職員等間でパスワードを共有してはならない。

第5章　技術的セキュリティ対策

第1節　コンピュータ及びネットワークの管理

(文書サーバの設定等)

第51条　情報システム管理者は、職員等が使用できる文書サーバの容量を設定し、必要に応じて職員等に周知しなければならない。

2　情報システム管理者は、必要に応じて文書サーバを課等の単位で構成しなければならない。

(バックアップの実施)

第52条　統括情報セキュリティ責任者及び情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

(システム管理記録及び作業の確認)

第53条　情報システム管理者は、所管する情報システムの運用において実施した作業について作業記録を作成しなければならない。

2　統括情報セキュリティ責任者及び情報システム管理者は、所管するシステムにおいて、変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

3　統括情報セキュリティ責任者、情報システム管理者又は情報システム担当者及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、2名以上で作業し、互いにその作業を確認しなければならない。

(情報システム仕様書等の管理)

第54条　統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう適切に管理しなければならない。

(ログの取得等)

第55条　統括情報セキュリティ責任者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

2　統括情報セキュリティ責任者及び情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

3　統括情報セキュリティ責任者及び情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

(障害記録)

第56条　統括情報セキュリティ責任者及び情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

（ネットワークの接続制御、経路制御等）

第 57 条　統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

2　統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

（外部ネットワークとの接続制限等）

第 58 条　情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO 及び統括情報セキュリティ責任者の許可を得なければならない。

2　情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、連合内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

3　情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

4　統括情報セキュリティ責任者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、連合内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

5　情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（複合機のセキュリティ管理）

第 59 条　統括情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

2　統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

（電子メールのセキュリティ管理）

第 60 条　統括情報セキュリティ責任者は、権限のない利用者により外部から外部への電子メール転送(電子メールの中継処理)が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

2　統括情報セキュリティ責任者は、大量のスパムメール等の受信又は送信を検知した場合はメールサーバの運用を停止しなければならない。

3　統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

4　統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

（電子メールの利用制限）

第 61 条　職員等は、自動転送機能を用いて、電子メールを転送してはならない。

2　職員等は、業務上必要のない送信先に電子メールを送信してはならない。

3　職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

4　職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

5　職員等は、ウェブで利用できるフリーメール、ネットワークストレージサービス等を使用してはならない。

（暗号化、パスワード設定）

第 62 条　職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

（無許可ソフトウェアの導入等の禁止）

第 63 条　職員等は、パソコン及びモバイル端末に無断でソフトウェアを導入してはならない。

2　職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

3　職員等は、不正にコピーしたソフトウェアを利用してはならない。

（機器構成の変更の制限）

第 64 条　職員等は、パソコン及びモバイル端末に対し機器の改造及び増設･交換を行ってはならない。

4　職員等は、業務上パソコン及びモバイル端末に対し機器の改造及び増設･交換を行う必要がある場合には、統括情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

（無許可でのネットワーク接続の禁止）

第 65 条　職員等は、統括情報セキュリティ責任者の許可なくパソコンをネットワークに接続してはならない。

（業務以外の目的でのインターネット閲覧の禁止）

第 66 条　職員等は、業務以外の目的でインターネットを閲覧してはならない。

2　統括情報セキュリティ責任者は、職員等のインターネット利用について明らかに業務に関係の閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適切な措置を求めなければならない。

第 2 節　アクセス制御等

（アクセス制御）

第 67 条　統括情報セキュリティ責任者又は情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

（利用者 ID の取扱い）

第 68 条　統括情報セキュリティ責任者及び情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、退職に伴う利用者 ID の取扱い等の方法を定めなければならない。

2　職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

3　統括情報セキュリティ責任者及び情報システム管理者は、利用されていない ID が放置されないよう、点検しなければならない。

（特権を付与された ID の管理等）

第 69 条　統括情報セキュリティ責任者及び情報システム管理者は、管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、

当該 ID 及びパスワードを厳重に管理しなければならない。

2　統括情報セキュリティ責任者及び情報システム管理者の特権を代行する者は、統括情報セキュリティ責任者及び情報システム管理者が指名し、CISO が認めた者でなければならない。

3　CISO は、代行者を認めた場合、速やかに統括情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

4　統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID 及びパスワードの変更について、外部委託事業者に行わせてはならない。

5　統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID 及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

6　統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。

(パスワードに関する情報の管理)

第 70 条　統括情報セキュリティ責任者又は情報システム管理者は、職員等のパスワードに関する情報を厳重に管理しなければならない。パスワードファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

2　統括情報セキュリティ責任者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

(職員等による外部からのアクセス等の制限)

第 71 条　職員等が外部から内部ネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

2　統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

3　統括情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

4　統括情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を施さなければならない。

5　統括情報セキュリティ責任者及びシステム管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

6　職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を連合内部のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認しなければならない。

7　統括情報セキュリティ責任者は、公衆通信回線(公衆無線 LAN 等)の外部通信回線を連合内のネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者の ID 及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体(IC カード等)による認証に加えて通信内容の暗号化等、セキュリティ確保のために必要な措置を講じなければならない。

（特権による接続時間の制限）

第 72 条　情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

第 3 節　システム導入、機器・ソフトウェア調達、保守等

（情報システム、機器・ソフトウェア等の調達）

第 73 条　統括情報セキュリティ責任者及び情報システム管理者は、システム導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

2　統括情報セキュリティ責任者及び情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

3　情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない

4　情報システム管理者は、システムの旧環境から新環境への移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

5　情報システム管理者は、導入するシステムの可用性が確保されていることを確認した上で、導入しなければならない。

（システム導入のテスト）

第 74 条　情報システム管理者は、新たにシステムを導入する場合、既に稼働しているシステムに接続する前に十分な試験を行わなければならない。

2　情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を実施しなければならない。

3　情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

（システム導入・保守に関連する資料等の整備・保管）

第 75 条　情報システム管理者は、システム導入・保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

2　情報システム管理者は、テスト結果を一定期間保管しなければならない。

3　情報システム管理者は、システムに係るソースコードを適切な方法で保管しなければならない。

（情報システムにおける入出力データの正確性の確保）

第 76 条　情報システム管理者は、情報システムに入力されるデータについて、範囲･妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

2　情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

3　情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

(情報システムの変更管理)

第 77 条　情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

(開発・保守用のソフトウェアの更新等)

第 78 条　情報システム管理者は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

(システム更新又は統合時の検証等)

第 79 条　情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新、統合後の業務運営体制の検証を行わなければならない。

第 4 節　不正プログラム対策

(統括情報セキュリティ責任者の措置事項)

第 80 条　統括情報セキュリティ責任者は、不正プログラム対策として、次の各号に掲げる事項を措置しなければならない。

(1)　外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、システムへの侵入を防止する。

(2)　外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、外部への拡散を防止する。

(3)　コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起する。

(4)　所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させる。

(5)　不正プログラム対策ソフトウェアのバージョンやパターンファイルは、常に最新の状態に保つ。

(6)　業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用しない。

(情報システム管理者の措置事項)

第 81 条　情報システム管理者は、不正プログラム対策に関し、次の各号に掲げる事項を措置しなければならない。

(1)　情報システム管理者は、その所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させる。

(2)　不正プログラム対策ソフトウェアのバージョンやパターンファイルは、常に最新の状態に保つ。

(3)　インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、本連合が管理している媒体以外を職員等に利用させない。また、不正プログラムの感染・侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェアのバージョン及びパターンファイルの更新を実施する。

(職員等の遵守事項)

第 82 条　職員等は、不正プログラム対策に関し、次の各号に掲げる事項を遵守しなければならない。

(1)　パソコンにおいて、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更しない。
(2)　外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行う。
(3)　差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除する。
(4)　端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施する。
(5)　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行う。
(6)　統括情報セキュリティ責任者が提供するウイルス情報を、常に確認する。
(7)　パソコン等がコンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、端末の LAN ケーブルの即時取り外しを行う。

(専門家の支援体制)

第 83 条　統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、必要に応じて外部の専門家の支援を受けられるようにしておかなければならない。

第 5 節　不正アクセス対策

(統括情報セキュリティ責任者の措置事項)

第 84 条　統括情報セキュリティ責任者は、不正アクセス対策として、次の各号に掲げる事項を措置しなければならない。
(1)　使用されていないポートを閉鎖する。
(2)　不要なサービスについて、機能を削除又は停止する。
(3)　不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定する。
(4)　統括情報セキュリティ責任者は、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築する。

(攻撃の予告)

第 85 条　CISO 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

(記録の保存)

第 86 条　CISO 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

(内部からの攻撃)

第 87 条　統括情報セキュリティ責任者及び情報システム管理者は、職員等及び外部委託事業者が使用しているパソコン等の端末からの連合内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

(職員等による不正アクセス)

第 88 条　統括情報セキュリティ責任者及び情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課等の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

（サービス不能攻撃）

第 89 条　統括情報セキュリティ責任者及び情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（標的型攻撃）

第 90 条　統括情報セキュリティ責任者及び情報システム管理者は、情報システムにおいて標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために通信をチェックする等の内部対策を講じなければならない。

第 6 節　セキュリティ情報の収集

（セキュリティホールに関する情報）

第 91 条　統括情報セキュリティ責任者及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（不正プログラム等に関する情報）

第 92 条　統括情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

（情報セキュリティに関する情報）

第 93 条　統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

第 6 章　運用

第 1 節　情報システムの監視

第 94 条　統括情報セキュリティ責任者及び情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

2　統括情報セキュリティ責任者及び情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

3　統括情報セキュリティ責任者及び情報システム管理者は、外部と常時接続するシステムを常時監視しなければならない。

第 2 節　情報セキュリティポリシーの遵守状況の確認

（遵守状況の確認及び対処）

第 95 条　情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに CISO 及び統括情報セキュリティ責任者に報告しなければならない。

2　CISO は、発生した問題について、適切かつ速やかに対処しなければならない。

3　統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

(パソコン等の利用状況調査)

第 96 条　CISO 及び CISO が指名した者は、不正アクセス･不正プログラム等の調査のために、職員等が使用しているパソコン及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

(職員等の報告義務)

第 97 条　職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告を行わなければならない。

第 3 節　侵害時の対応等

(緊急時の対応)

第 98 条　CISO は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施しなければならない。

第 4 節　例外措置

(例外措置の許可)

第 99 条　情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合には、CISO の許可を得て、例外措置を取ることができる。

(緊急時の例外措置)

第 100 条　情報セキュリティ管理者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに CISO に報告しなければならない。

(例外措置の申請書の管理)

第 101 条　CISO は、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

第 5 節　法令遵守

第 102 条　職員等は、職務の遂行において使用する情報資産を保護するために、次の各号に掲げる法令のほか関係法令を遵守し、これに従わなければならない。

(1)　地方公務員法(昭和 25 年法律第 261 号)
(2)　著作権法(昭和 45 年法律第 48 号)
(3)　不正アクセス行為の禁止等に関する法律(平成 11 年法律第 128 号)
(4)　個人情報の保護に関する法律(平成 15 年法律第 57 号)
(5)　行政手続における特定の個人を識別するための番号の利用等に関する法律(平成 25 年法律第 27 号)
(6)　サイバーセキュリティ基本法(平成 26 年法律第 104 号)
(7)　相楽東部広域連合個人情報保護条例(平成 21 年条例第 2 号)

第 6 節　懲戒処分等

(懲戒処分)

第 103 条　情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法(昭和 25 年法律第 261 号)による懲戒処分の対象とする。

（違反時の対応）

第 104 条　職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の各号に掲げる措置を講じなければならない。

(1)　統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課等の情報セキュリティ管理者に通知し、適切な措置を求める。

(2)　情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員等が所属する課等の情報セキュリティ管理者に通知し、適切な措置を求める。

(3)　情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後、統括情報セキュリティ責任者は、速やかに職員等の権利を停止あるいは剥奪した旨を CISO 及び当該職員等が所属する課等の情報セキュリティ管理者に通知する。

第 7 章　外部サービスの利用

第 1 節　外部委託

（外部委託事業者の選定基準）

第 105 条　情報セキュリティ管理者は、外部委託事業者の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

2　情報セキュリティ管理者は、クラウドサービスを利用する場合は情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

（契約項目）

第 106 条　情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の各号に掲げる情報セキュリティ要件を明記した契約を締結しなければならない。

(1)　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

(2)　委託事業者の責任者、委託内容、作業者及び作業場所の特定

(3)　提供されるサービスレベルの保証

(4)　外部委託事業者にアクセスを許可する情報の種類と範囲及びアクセス方法

(5)　外部委託事業者の従業員に対する教育の実施

(6)　提供された情報の目的外利用及び受託者以外の者への提供の禁止

(7)　業務上知り得た情報の守秘義務

(8)　再委託に関する制限事項の遵守

(9)　委託業務終了時の情報資産の返還・廃棄等

(10)　委託業務の定期報告及び緊急時報告義務

(11)　連合による監査及び検査

(12)　連合による情報セキュリティインシデント発生時の公表

(13)　情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

（確認・措置等）

第 107 条　情報セキュリティ管理者は、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて前条の契約に基づき措置しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じて CISO に報告しなければならない。

第2節　約款による外部サービスの利用

(約款による外部サービスの利用に係る規定の整備)

第108条　情報セキュリティ管理者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、重要性Ⅱ以上の情報が取り扱われないように規定しなければならない。

(1)　約款によるサービスを利用してよい範囲

(2)　業務により利用する約款による外部サービス

(3)　利用手続及び運用手順

(約款による外部サービスの利用における対策の実施)

第109条　職員等は、利用するサービスの約款、その他提供条件から利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

第3節　ソーシャルメディアサービスの利用

第110条　情報セキュリティ管理者は、本連合が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の各号に掲げる事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

(1)　本連合のアカウントによる情報発信が、実際の本連合のものであることを明らかにするために、本連合の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自己記述欄等にアカウントの運用組織を明示する等の方法で、なりすまし対策を行うこと。

(2)　パスワードや認証のためのコード等の認証情報及びこれを記録した媒体等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

2　重要性Ⅱ以上の情報はソーシャルメディアサービスで発信してはならない。

3　利用するソーシャルメディアサービスごとの責任者を定めなければならない。

第8章　評価・見直し

第1節　監査

(監査の実施方法)

第111条　CISOは、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、必要に応じて監査を行わせなければならない。

(監査を行う者の要件)

第112条　情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部署から独立した者に対して、監査の実施を依頼しなければならない。

2　監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

(監査実施計画の立案及び実施への協力)

第113条　情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、CISOの承認を得なければならない。

2　被監査部署は、監査の実施に協力しなければならない。

（外部委託事業者に対する監査）

第 114 条　外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請として受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的に、又は必要に応じて行わなければならない。

（監査報告）

第 115 条　情報セキュリティ監査統括責任者は、監査結果を取りまとめ CISO 及び委員会に報告する。

（保管）

第 116 条　情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠及び監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

（監査結果への対応）

第 117 条　CISO 及び委員会は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

（情報セキュリティポリシー及び関係規程等の見直し等への活用）

第 118 条　CISO 及び委員会は、監査結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

第 2 節　自己点検

（自己点検の実施方法）

第 119 条　統括情報セキュリティ責任者及び情報システム管理者は、所管するネットワーク及び情報システムについて必要に応じて自己点検を実施しなければならない。

2　情報セキュリティ管理者は、所管組織における情報セキュリティポリシーに沿った情報セキュリティ対策状況について必要に応じて自己点検を行わなければならない。

（自己点検報告）

第 120 条　統括情報セキュリティ責任者及び情報システム管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、CISO 及び委員会に報告しなければならない。

（自己点検結果の活用）

第 121 条　職員等は、自己点検の結果に基づき自己の権限の範囲内で改善を図らなければならない。

2　CISO 及び委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない

第 3 節　情報セキュリティポリシー及び関係規程等の見直し

第 122 条　CISO 及び委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、情報セキュリティポリシー及び関係規程等について、毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めたときは、改善を行うものとする。

附　則

この要綱は、令和３年８月１日から施行する。